UNIVERSAL SECURITY EXHIBIT

This Workday Universal Security Exhibit applies to the Covered Service and Covered Data. Capitalized terms used herein have the meanings given in the Agreement, including attached exhibits, that refers to this Workday Universal Security Exhibit.

Workday maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of Covered Data as well as the associated risks, are appropriate to (a) the type of information that Workday will store as Covered Data; and (b) the need for security and confidentiality of such information. Workday's security program is designed to:

- Protect the confidentiality, integrity, and availability of Covered Data in Workday's possession or control or to which Workday has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Covered Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Covered Data;
- Protect against accidental loss or destruction of, or damage to, Covered Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Workday may be regulated.

Without limiting the generality of the foregoing, Workday's security program includes:

1. **Security Awareness and Training**. Mandatory employee security awareness and training programs, which include:

   a) Training on how to implement and comply with its information security program; and

   b) Promoting a culture of security awareness.

2. **Access Controls**. Policies, procedures, and logical controls:

   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

   b) To prevent those workforce members and others who should not have access from obtaining access; and

   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the data centers housing Covered Data is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any security breach of any application or system directly associated with the accessing, processing, storage or transmission of Covered Data.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Covered Data or production systems that contain Covered Data.

6. **Audit Controls**. Technical or procedural mechanisms put in place to promote efficient and effective operations, as well as compliance with policies.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Covered Data and to protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Covered Data that is being transmitted over a public electronic communications network or stored electronically.

©2019 Workday 19.5

UNIVERSAL SECURITY EXHIBIT

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Covered Data, taking into account available technology so that such data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its information security program, including:

    a) Designating a security official with overall responsibility; and

    b) Defining security roles and responsibilities for individuals with security responsibilities.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

    a) Reviewing changes affecting systems handling authentication, authorization, and auditing;

    b) Reviewing privileged access to Workday production systems processing Covered Data; and

    c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Workday makes to production systems, applications, and databases processing Covered Data. Such policies and procedures include:

    a) A process for documenting, testing and approving the patching and maintenance of the Covered Service;

    b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

    c) A process for Workday to utilize a third party to conduct web application level security assessments. These assessments generally include testing, where applicable, for:

        i) Cross-site request forgery

        ii) Services scanning

        iii) Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)

        iv) XML and SOAP attacks

        v) Weak session management

        vi) Data validation flaws and data model constraint inconsistencies

        vii) Insufficient authentication

        viii) Insufficient authorization

14. **Program Adjustments**. Workday monitors, evaluates, and adjusts, as appropriate, the security program in light of:

    a) Any relevant changes in technology and any internal or external threats to Workday or the Covered Data;

    b) Security and data privacy regulations applicable to Workday; and

    c) Workday's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

©2019 Workday 19.5